VMware Solutions for the Connected Car

Version 1.0

April 2015

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Contents

1. Challenges and Use Cases for Connected Cars

As the value proposition of vehicle manufacturers moves from a product-centric to a customer-centric approach, technology leadership—according to Gartner—will determine the future of the automotive industry. Access to cloud and data resources, as well a real time analytics, is imperative to support 250 million connected cars by the year 2020[1]. Once established, these technologies will help to propel the automotive industry to the connected car, the connected driver, and ultimately, to the connected consumer industry (the Internet of Things). This will open a variety of new business opportunities that extend into many adjacent industries.

While more and more functionality is achieved by offloading it to connected consumer devices in the form of smartphones or tablets, basic functionality must still be available even if the external device is not available[2]. This increases the future importance of the built-in head unit and other integrated systems and installed software as the main point of interaction between driver and vehicle. Drivers today are familiar with the functionality of their smartphones and expect to have the same features and functionality—application availability, operating system, and updates over-the-air. This will in turn increase the value of the vehicle to its current and possible future owners.

In a connected world, the vehicle is no longer self-contained, but relies on services provided by an OEM vehicle back end that serves as the vehicle's interface to the online world[3]. The OEM vehicle back end creates a virtual image of the vehicle in cyber space and must provide highest level of IT and data security. At the same time, the back end must be flexible and scalable enough to accommodate loads created by stochastic user and device behavior. To provide such features, the back-end systems can no longer be manually assembled in a custom fashion, but must be highly integrated and automated to guarantee the highest quality, lowest possible failure rate, 24/7 availability, and fastest time-to-market.. All alterations to such back end systems, whether compute, network, security, or storage, must be logged in an auditable fashion.

The combination of vehicle back end, over-the-air head unit control, and probable connection to electronic control units (ECUs), enables a new quality in provided services. These can be categorized into the two main groups of 1) customer relationship management, including after-sales predictive maintenance and after-sales customization, and 2) vehicle relationship management that enables information feedback about feature usage patterns to product management and sales.

VMware customer-proven technologies can be used to build a highly scalable and secure vehicle backend with real time analytics and over-the-air update capabilities. This paper investigates these technologies and provides example use cases and key takeaway summaries.

[1] http://www.gartner.com/newsroom/id/2970017

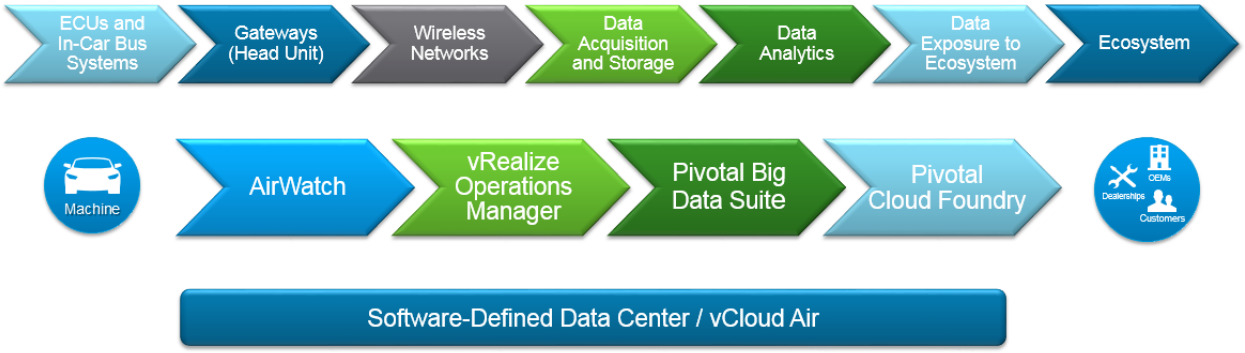
[2] Kohler, Stümpfle: „Die Konnektivität als Kernmerkmal von Premiumfahrzeugen“ / Springer, Industrie 4.0, ISBN-10:3-642-36916-2

[3] ibid

2. VMware Approach to the Connected Car Value Chain

A comprehensive vision of the connected car value chain involves multiple stakeholders, from the automobile itself to the OEMs, dealerships, services, and drivers. A viable connected car vision requires the involvement and integration of multiple components to efficiently collect telemetry data from cars and to perform remote provisioning of software packages, apps, and updates.

Figure 1. VMware Vision of the Connected Car Value Chain



Multiple connected car strategies can be implemented on top of the VMware technology stack displayed above, leveraging products such as AirWatch® for head unit management and remote control, VMware vRealize™ Operations Manager™ for telemetry data acquisition and analytics, Pivotal Big Data Suite for trend analysis, and Pivotal Cloud Foundry as the platform as a service (PaaS) component.

3. Car Management with AirWatch Mobile Device Management

AirWatch Mobile Device Management was developed to help organizations that deploy smartphones, tablets, and laptops in a secure and effective way to enable a mobile workforce and improve employee productivity. Today AirWatch manages millions of devices worldwide, from the cloud or on premise. The AirWatch platform is built on a highly scalable, multitenant architecture that allows organizations to securely deploy corporate email, apps, documents, and internal content to their workforce, and to comply with security standards across the entire mobile device fleet. Recently, AirWatch capabilities were extended to support Internet of Things (IoT) applications by managing wearables (such as smart watches, mobile printers, and dispensers) and additional embedded devices requiring over-the-air data collection and provisioning.

Mobility is the raison d'être of the automotive industry, so modern cars can be considered mobile devices on wheels, embedding dozens of engine control units (ECU) running up to 100 million lines of code, interconnected by vehicle bus systems and gateways. As a result, in-car electronics represent a significant amount of a modern automobile's R&D and production costs. The car's head unit, originally designed as the front end for the vehicle's audio system, has been expanded over the years to deliver value-added connected services such as navigation, real time traffic information display, diagnostic information and alerts, in addition to user-centric data such as emails, social feeds, and weather information.

The head unit can therefore be considered a mobile device, typically running a real-time operating system such as QNX[4], with all the well-known challenges of over-the-air data collection and software provisioning known from the mobile device world. QNX is an operating system designed for connected embedded systems, including ARM and x86, and boards implemented in virtually every type of embedded environment. It offers a highly customizable, modular operating system for use in multiple industries and systems. Its flexibility and robustness makes QNX a strong candidate for the automotive industry[5].

Key Takeaway 1: The head unit is a mobile device with challenges regarding secure over-the-air data collection, over-the-air software provisioning, and security similar to smartphones and tablets.

Head unit management opens the road for strong, innovative value-added services that can benefit the entire automotive ecosystem (OEMs, dealers, services, drivers). This is possible thanks to the three main pillars of the management framework:

- Over-the-air remote car data collection
- Over-the-air remote data and content provisioning
- Data security and privacy

3.1 Over-the-Air Data Collection

Access to critical car diagnostic data is a key challenge for the automotive industry. In most modern cars, diagnostic data are first collected when the car is serviced. A computer connected using an industry-standard on-board diagnostic (OBD-II) cable is required for OEMs to obtain sensor data, engine status, breakdown reports, wear and tear information, driving habits, and the like. Not being able to remotely access diagnostic data is a big burden for OEMs because they are unable to proactively detect software or hardware flaws. This often leads to expensive car recalls, increased numbers of warranty cases, and

[4] http://www.qnx.com/products/neutrino-rtos/index.html

[5] Fortune, "QNX: The little-known company that controls your car." Kurt Wagner, April 13, 2013 http://for.tn/1tsZloq

high rates of customer dissatisfaction. In addition, drivers have few to no options for interacting with their car remotely and obtaining valuable information such as location, alerts, battery charge status, and mileage to the next service. There are no industry standards, and therefore no end-to-end solutions for remotely collecting telemetry data. The different stakeholders in the connected car value chain do not work together to integrate all involved systems and build flexible and scalable solutions. Because of this, open source community-driven efforts are beginning to appear.

The VMware IoT agent running on the head unit can collect customizable sets of data (metrics) and report them to back-end systems over secure channels in real time. Because the head unit acts as gateway, metrics from ECUs and sensor data are obtained over the various car communication bus systems (such as CAN, FlexRay, and MOST) and securely stored in the agent's local database. Remote collection of these metrics occurs over a secure channel established on one of following wireless networks:

- Cellular network through embedded SIM card (in head unit or dedicated ECU)
- Cellular network by way of the driver's smart phone
- WiFi network (home network or public hot spots)

Metrics are stored and inventoried in the back end and can be used for further processing. Combined with VMware vCloud® Air™ hybrid cloud, this system easily scales with growing demands. This is so historical metrics from millions of cars can be collected, stored, and processed simultaneously and securely at optimal cost. VMware™ vRealize Operations Manager™ self-learning tools, predictive analytics, and smart alerts, enable proactive identification and possible remediation of emerging issues.

Use Cases

- Preventive diagnostics
- Dealership services
- Adaptive insurance services
- Reporting campaigns for early defect detection
- Service notifications
- ECU issue notifications
- Burglar alarm
- Car localization
- Notifications of oil and tire pressure loss and low battery conditions

Key Takeaway 2: The VMWare IoT agent running on the head unit can collect telemetry data and transmit it over a secure channel to a scalable back end.

3.2 Over-the-Air Data and Content Provisioning

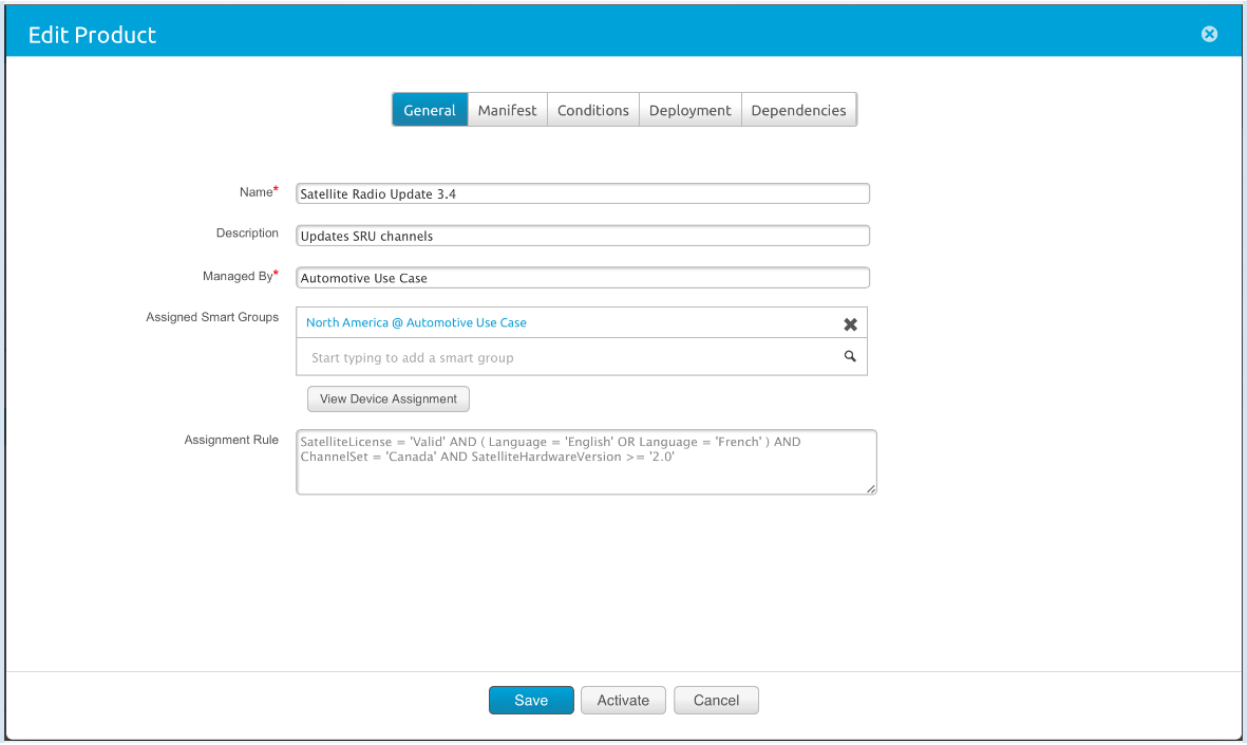
The ability to push data and content over-the-air to cars creates a new road for innovative value-added services and features in the connected car world.

3.2.1 Firmware Upgrades

Similar to smartphones and tablets, the head unit's firmware requires upgrades to enable new functionality and adapt to customer's expectations. Why should a driver be required to drive to a dealership for maintenance if he can get the latest head unit features over-the-air? The AirWatch product provisioning feature allows pushing a software upgrade to the head unit in a few clicks from the AirWatch console. A "product" is a set of files, actions, conditions, assignments, deployment options and dependencies allowing the provisioning of software packages to a car. Specific subsets of cars can be targeted through flexible assignment rules, for example "all model *x* cars in made for the German market

with head units running firmware version 2.0 and earlier." As an extension of this workflow, firmware upgrades might be pushed to individual ECUs to fix software bugs and avoid expensive significant car recalls.

Figure 2. Sample Product for Satellite Radio Update on Head Unit in the AirWatch Console



3.2.2 Remote Command and Control

As IoT matures, people expect to remotely command and control connected objects. Remote car lock/unlock, A/C setup, and car finder and charging management for electric vehicles are features launched by some of the most innovative car manufacturers in recent years. These features require that the entire value chain to be integrated and multiple components, from vehicle ECUs to back-end application and database servers, to interact flawlessly. Complexity and integration costs increase as more technologies are integrated. Combining AirWatch product provisioning and scalable API framework with the VMware software-defined data center (SDDC) and analytic tools allow OEMs to build a sustainable connected car strategy for the future.

3.2.2.1. Use Cases

- Remote car lock/unlock
- Remote A/C setup/pre-heat/cooling
- Find my car

3.2.3 Apps, Content, and User Profile Deployment

Mobile apps enhance our everyday life, quality, and productivity. Ubiquitous and secure access to content (email, documents, media) is the core of today's connected world. As cars become more and more connected, drivers are expecting app and content delivery to be as flexible as on their smartphones and tablets. The AirWatch mobile application and content management can be used to remotely provision

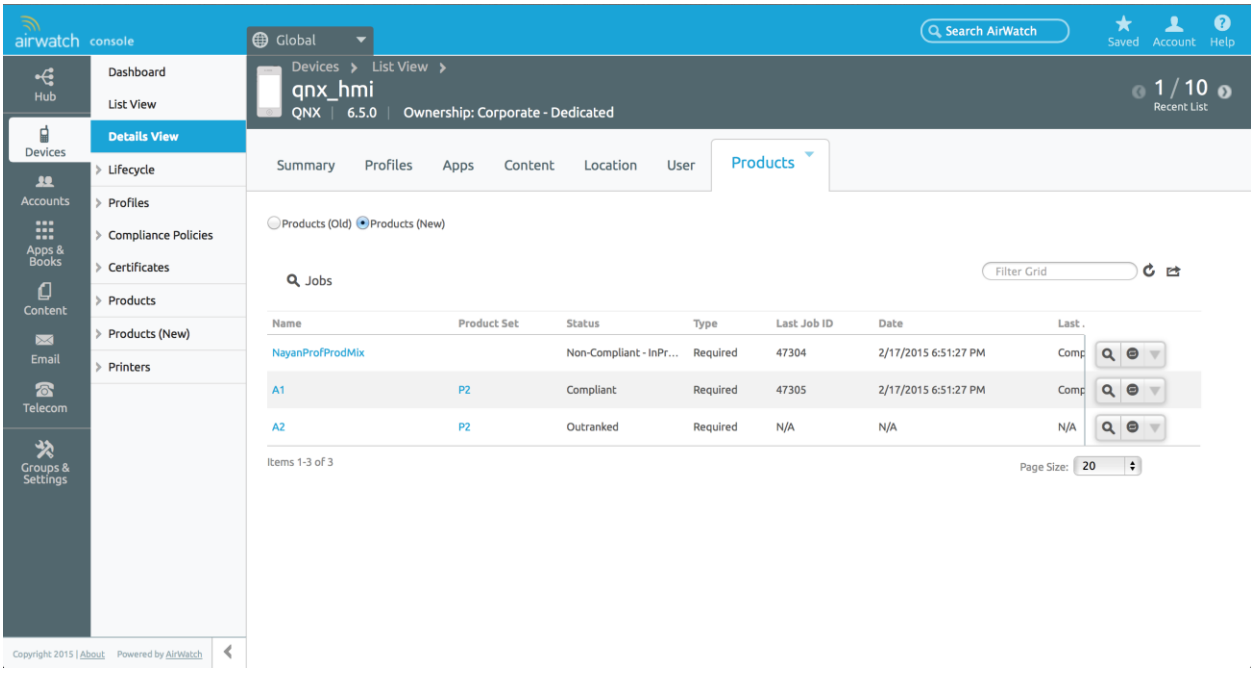
apps, music, video, diaries, mail, and documents to the head unit. In this way, drivers get a seamless experience from their smart devices into their cars.

As car sharing services become more and more popular around the world, technological challenges for delivering a scalable service become higher. Hardware customization is required for a car to join a car sharing pool, be unlocked, and tracked remotely. In addition, drivers expect their preferences, music, and favorite navigation routes to travel with them as they switch cars. AirWatch multi-user mode and product provisioning can be used to unlock the car, push the user's context, and start the billing cycle remotely, without additional hardware customization.

Use Cases

- Provisioning of the drivers' music and video playlists to the car's infotainment system
- Provisioning of GPS routes and points of interest
- Remote installation and upgrade of apps for accessing emails, social feeds, news, weather, and traffic information
- Remote provisioning of the driver's personal context
- Securely de-provisioning and wiping of downloaded content upon return of the vehicle

Figure 3. Device Inventory and Product Provisioning in the AirWatch Console



3.2.4 Post-Sales Car Customization and Self-Service Portal

Car manufacturers today offer dozens of optional accessories, functionality, and equipment to their customers, involving hardware and software customization. In some cases, expensive production line customization is required to support options available in car configurators. As software is gaining increasing importance in modern cars, it becomes conceivable to remotely activate some of the car's optional equipment and functionality postproduction, over-the-air. AirWatch product provisioning allows post-production car customization and flexible activation and deactivation of features on the head unit. Additionally, drivers and fleet managers have very few options today to receive alerts, consumption information, and cost figures from their cars. The AirWatch self-service portal is an ideal tool to enable

them to interact remotely with their cars. A new set of value propositions for the whole ecosystem can emerge.

Use Cases

- Post-production car customization to avoid expensive production line customization.
- Delivery of new options and upgrades to older car models for additional revenue.
- Pay-as-you-use model for drivers to use some options for a specific amount of time (enhanced navigation, real time traffic information, audio surround system, and horsepower on demand).
- Self-service portal for drivers and fleet managers to obtain valuable information about their cars and provide real-time tips on how to improve efficiency and consumption.

Key Takeaway 3: Over-the-air head unit software provisioning allows innovative services and use cases to be developed by the automotive ecosystem.

3.3 Data Security and Privacy

Telemetry data, especially in a user-driven context, can be sensitive and require solid privacy and security considerations. Type and frequency of data collected needs to be customizable as well as encrypted end-to-end. Some data required for predictive analysis must not be displayed or made available to third parties because that could allow the profiling of a user's behavior. To address security and privacy challenges, the AirWatch platform is built with industry-standard FIPS 140-2 algorithms and relies on a strong privacy engine, which enables the customization of collected and stored data types.[6] The head unit's IoT agent can store data in an encrypted container and transmit it to the data center over secure channels. The containerization concept, well known in the enterprise mobility management industry for separation of corporate and private data, addresses the challenges of security and privacy across the entire value chain.

[6] VMware white paper: "Protecting Sensitive Government Data on Mobile Devices: Maintaining FIPS 140-2 Compliance," 2014. Available for download: http://www.air-watch.com/downloads/resources/Protecting_Sensitive_Government_Data_on_Mobile_Devices_20140718.pdf

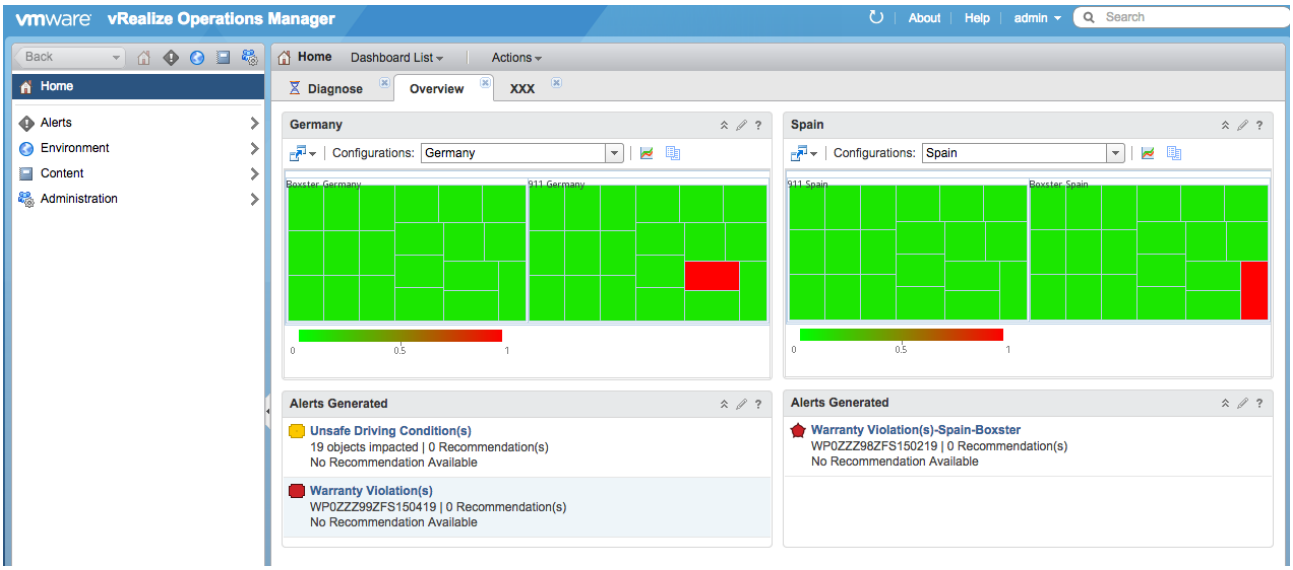
4. vRealize Operations Manager for Data Collection and Analysis

Traditional operations management systems do not meet the requirements of today's virtual and cloud infrastructures. They make IT too reactive because they lack the intelligence to aggregate, correlate, and analyze metrics across applications and infrastructure stacks. VMware vRealize Operations Manager is built on a scale-out, resilient platform that delivers intelligent operational insights to simplify and automate management of applications and infrastructure in one place.

4.1 Project Helix Brings vRealize Operations Manager to the Internet of Things

At its core, vRealize Operations Manager is a telemetry acquisition and analysis tool. Project Helix is a recently created incubator program at VMware. The project proposes to bring the mature function in vRealize Operations Manager for data center objects to telemetry data collected from external devices. Inherent in this approach is the abstraction that IoT edge-aggregation systems (such as the head unit in a vehicle) can be considered as *just another data source*, albeit one with many more metrics to stream and a much higher scaling factor. With this abstraction, not only vRealize Operations Manager, but also other management tools, such as VMware vRealize™ Log Insight™, can be used with IoT edge-aggregation systems. The current release of vRealize Operations Manager greatly expands the componentization of the core engine, providing for pluggable adapters (which define the communications between external devices, the look and feel of the GUI, actions, alert types, symptom types, and the like) and a complete public, documented REST API, which allows programmatic access to all engine features.

Figure 4. vRealize Operations Manager Dashboard with Sample Conditions and Violations



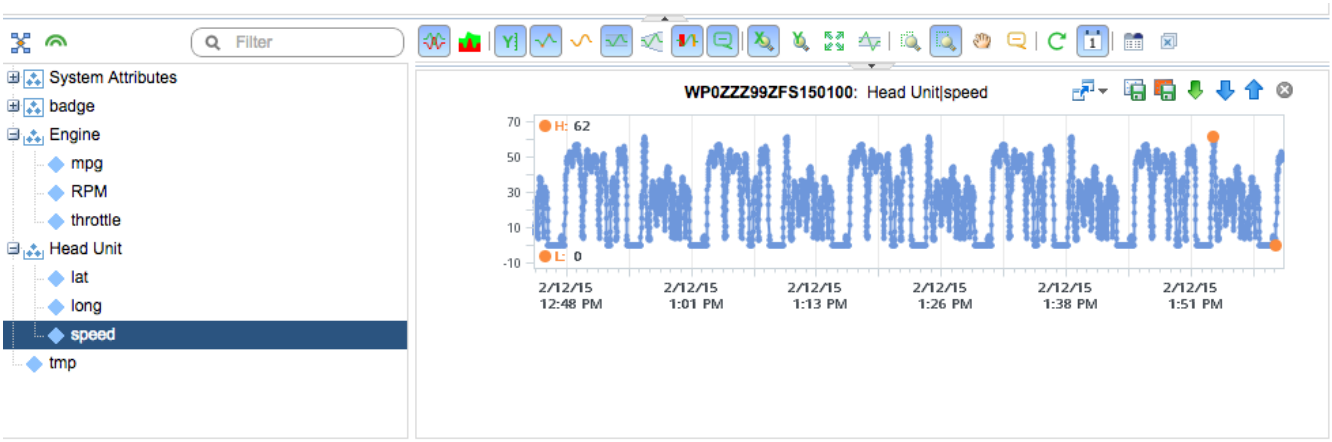
Project Helix comprises three major components:

- VMware software-defined data center and vCloud Air as scalable, highly resilient, and available infrastructure
- vRealize Operations Manager to collect telemetric data from devices, organize views of the devices and date, analyze incoming real time streams, issue user defined and commands, and raise alerts
- A device agent to aggregate data from sensors and execute commands from vRealize Operations Manager

Project Helix is building an IoT-specific adapter targeted at collection of high-volume streams of telemetry data from millions of devices, programmatic device-defined actions, IoT-specific organizational schemes, and secure communications channels.

One of the many advantages of using vRealize Operations Manager for IoT telemetry acquisition is the ability for devices to use up to eight fields to create a unique identifier representing itself in vRealize Operations Manager. The creation of this universally unique identifier (UUID) is a protocol between the device and in instance of vRealize Operations Manager that is driven completely by the device. During initial registration, the device receives error codes from vRealize Operations Manager if its choice of input values is not unique among all of the currently registered devices in this vRealize Operations Manager instance. The device can then add, modify, and experiment with values in the fields to become unique. For example, some of the fields might be year of manufacture, serial number, media access control (MAC) addresses, location coordinates, and so forth. After this UUID is created, all communication between the device and vRealize Operations Manager need only contain the UUID.

Figure 5. Historical Telemetry Data in vRealize Operations Manager



Most importantly, no pre-configuration of vRealize Operations Manager is necessary—devices essentially can configure themselves in vRealize Operations Manager. No global naming authority is necessary to give devices unique identifiers. All the uniqueness happens dynamically at runtime.

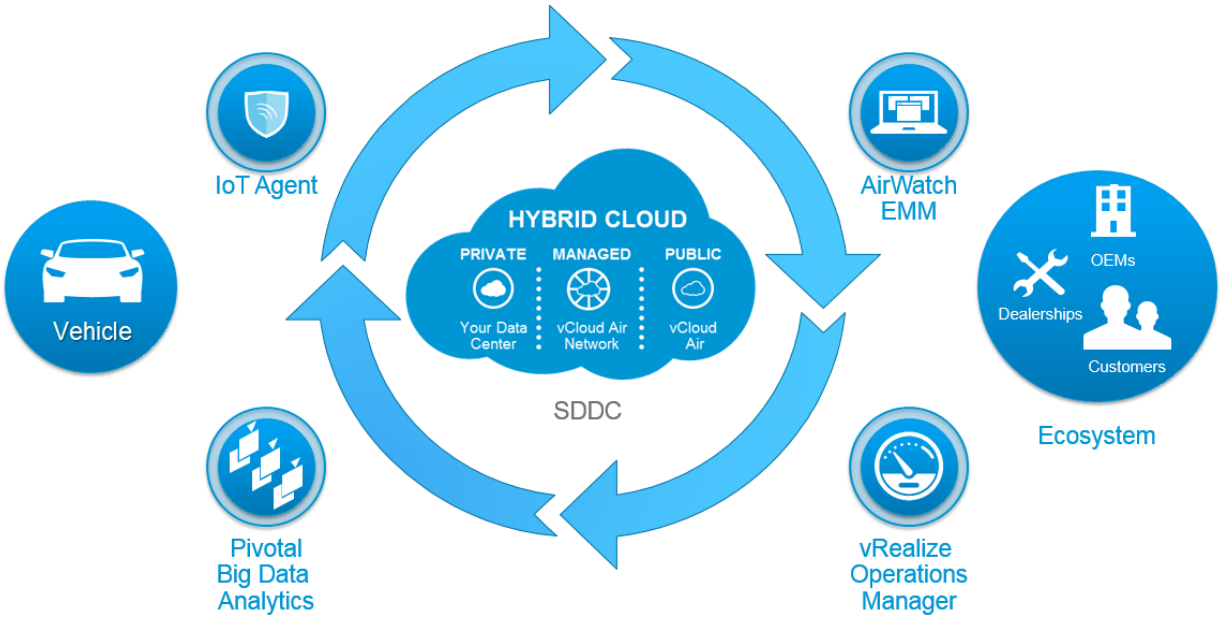
This feature will allow scaling and ease of device deployment potentially useful for the automotive industry. For example, vRealize Operations Manager can easily be configured to monitor the oil level in vehicles, notify the owner if the oil level falls below recommended values, notify the owner if the recommended interval for oil changes has been exceeded, and notify the warranty division when recommended intervals are ignored.

Key Takeaway 4: vRealize Operations Manager delivers self-learning tools, predictive analytics, and smart alerts enabling proactive identification and remediation of emerging issues. Project Helix is the vRealize Operations Manager extension to the IoT world and more specifically, to the automotive industry.

5. The Software-Defined Data Center as Backbone

In conjunction with the VMware hybrid cloud—vCloud Air—the software-defined data center (SDDC) provides a limitless, dynamic, and scalable vehicle back end. All systems within the SDDC are created automatically with only minimal human intervention, using pre-defined blue prints that contain all information about compute, network, security, and storage and therefore make it easy to create and re-create systems, while being fully auditable. Built-in high availability and fault tolerance enable 24/7 operations without downtime. The hybrid cloud approach provides “breathing space” to accommodate load created by stochastic user behavior, and it scales on demand, for example, for the launch of new product features. The operations management system within the SDDC continuously analyzes thousands of system parameters to provide predictive maintenance information. The following diagram pictures the high-level end-to-end solution built on top of the VMware technology stack for the connected car ecosystem.

Figure 6. Data Flow from Car to Ecosystem and Back



Key Takeaway 5: The massive amount of data created by connected devices cannot be handled in a traditional hardware-defined data center approach. A software-defined approach with hybrid cloud option can scale quickly to meet these data requirements.

6. Future Research Perspectives

6.1 ARM CPU Support

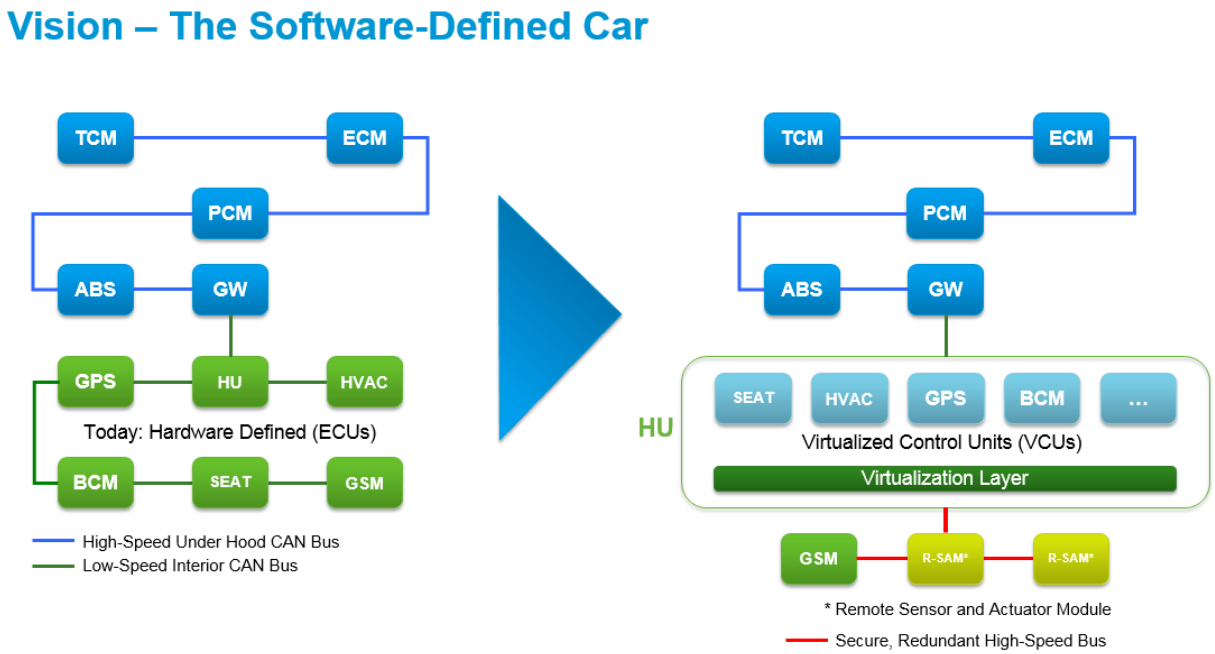
VMware, the recognized leader in x86 virtualization, is now closely following developments in ARM's technology ecosystem and has a team dedicated to porting the VMware ESXi™ hypervisor to the ARM8 architecture. There is currently insufficient server market demand to justify releasing this as part of a product portfolio, however, VMware is very interested in exploring new market opportunities with customers and partners in the embedded space to help shape strategy moving forward. There are use cases in the area of providing high availability and fault tolerance for systems related to automated/driverless driving, and in providing a flexible way to use the compute power of head units by securely separating applications through virtualization.

6.2 Vision: The Software-Defined Car

VMware has shown that the software-defined approach has many advantages for data centers as differentiating intelligence has moved from dedicated hardware to software run on less task-specific hardware. VMware introduced compute virtualization many years ago and virtualization has since become mainstream, dramatically increasing server utilization while maintaining consistent response time. VMware is now able to virtualize networks as well. VMware helps the telecommunication industry to virtualize functions that up until now have been provided by highly specialized appliances. This is called network function virtualization, or NFV. However, VMware takes this a step further and virtualizes every function of IP networks using VMware NSX™. This approach radically simplifies the network across the entire data center and provides unprecedented security by easily microsegmenting the various virtual components.

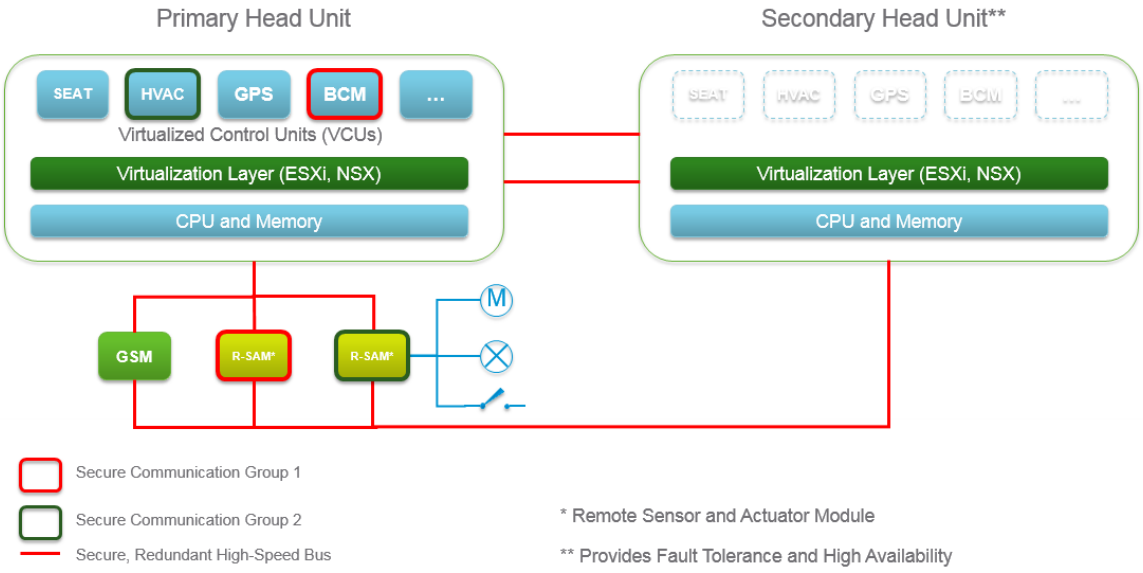
VMware can apply the same principles to automobile electronic components. The VMware approach is to virtualize the functions, which today reside in specialized ECUs, the same way network functions for the telecom industry were virtualized—the software from the ECU is virtualized, thus becoming a virtualized control unit (VCU).

Figure 7. From ECUs to VCUs



These VCUs would then run on a specialized version of the VMware ESXi virtualization layer inside the head unit, which becomes the centerpiece and provides the compute power. The sensors and actuators, which in the classical approach are connected to the ECU, would then have to be connected to a simple and universal controller, called the Remote Sensor and Actuator Module, or R-SAM. It ideally provides several analog and digital inputs as well as outputs for light or motor control, which can be configured in a way analogous to LEGO toy building bricks. These modules then communicate with their virtualized counterparts through a redundant high-speed bus, possibly even fiber optics, whereby the communication between the components is secured by micro-segmentation and firewalls. This approach to security will make it extremely difficult for attackers to hijack the systems even if they do gain access to the vehicle's systems. While this architecture might not be immediately viable for systems concerned with driving safety (such as anti-lock braking system [ABS], power-train control module [PCM], or airbag control unit [ACU]), it will certainly be able to replace most of the systems used today in the area of passenger convenience, entertainment, and navigation. Besides a radically simplified cabling and logical design allowing for lower failure rates, the benefits provide savings by reducing the number of copper-based busses, such as controller area network (CAN). Furthermore, easier software updates are possible because the software is now running on a virtualized platform for which proven update mechanisms exist. This also enables the introduction of new features to the aftermarket. Another benefit of virtualization is that various operating systems can run side by side on one head unit, providing much higher flexibility for the manufacturer to pick and choose. An additional level of safety can be introduced by having a secondary head unit residing in a physically different location, such as the trunk. Standard mechanisms within the virtualization layer would then provide seamless failover in case one of the head units is destroyed or fails for other reasons.

Figure 8. Redundancy for Better Reliability in the Software-Defined Car



Key Takeaway 6: Proven approaches and concepts from the software-defined data center are worth being explored in the area of connected cars.

6.3 AUTOSAR and ESXi

The AUTOSAR[7] partnership to which many OEMs and suppliers belong brought AUTOSAR to life in 2003 as a platform to unify the programming model and the runtime system for ECUs. It can be compared to the platform component in a PaaS stack. AUTOSAR is not a product, but a specification to which OEMs and their suppliers may or may not conform, which is one of the reasons AUTOSAR has not been fully and widely adopted. AUTOSAR has only recently added support for multicore CPUs and a TCP/IP stack. It does not provide isolation levels for communication between ECUs, nor does it support fault tolerance. In fact, code executing on the AUTOSAR runtime must implement fault tolerance itself. This is not only a major undertaking, but it is also error prone and would have to be adapted to each new processor architecture. Alternatively, the VMware ESXi hypervisor has supported multicore CPUs and fault tolerance through software lock stepping for many years, and the NSX networking components provide microsegmentation and security in the most demanding environments. Thus, VMware ESXi combined with software lockstepping and NSX is the ideal underpinning for the AUTOSAR runtime, adding easy portability, fault tolerance, isolation among virtual machines, and network security, without the need to change the application.

[7] http://www.autosar.org